UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,895	02/28/2002	Ted Christian Johnson	10017900-1	2863

7590 09/09/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
PEARSON, DAVID J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/085,895	JOHNSON, TED CHRISTIAN	
	Examiner	Art Unit	
	David J. Pearson	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 June 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20050808*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

1. Claims 1-28 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-2, 4, 8, 11-12, and 17-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al. (U.S. Patent 6,374,359), and further in view of Rail (Patent Application Publication 2003/0110399) and Shibata et al (U.S. Patent 5,586,185).

For claims 1, 17 and 21, Shrader et al. teach a method for authenticating a web session comprising: receiving a user ID (note column 5, lines 44-50); encrypting a message using an encryption key (note column 7, lines 21-23); and converting the encrypted message into an ASCII string (note column 7, lines 33-36).

Shrader et al. differ from the claimed invention in that they fail to specify: computing a message digest of the user ID; computing an expiration timestamp for the session; and combining the message digest and expiration timestamp.

Rail teaches a similar device as Shrader et al. in which, a message digest of the user ID is computed (note paragraph [0036]); an expiration timestamp for the session is computed (note paragraph [0032]); and the message digest and expiration timestamp are combined (note paragraph [0036]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the device of Shrader et al. using the methods of Rail for the added securities of knowing the cookie has not been tampered with (message digest) and the cookie is not being used after a given length of time has elapsed (timestamp).

The combined invention of Shrader et al. and Rail differ from the claimed invention in that they fail to specify: selecting an index number; accessing an encryption key using the index number; and encrypting the message using the accessed encryption key.

Shibata et al. teach a communication method in which encryption keys are stored in table with an index number. When sending a message, the user selects an index number (note column 10, lines 43-51), the encryption key is accessed using the index number and the message is encrypted using the selected key (note column 18, lines 54-64).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the inventions of Shrader et al. and Rail with the encryption method of Shibata et al. Rail teaches the use of "any suitable private encryption key" and Shrader et al. teach "preferably, the key pair is constructed and stored locally (for root user access only) during configuration of the Web server." The method of Shibata et al. meets these qualifications and teaches improved key management through "a 'cipher key table' in which a plurality of cipher keys and their index numbers are updatably registered."

For claims 2 and 22, the combination of Shrader et al., Rail and Shibata et al. teach a method of claims 1 and 21, wherein the step of combining the message digest and expiration timestamp more specifically includes concatenating the message digest and expiration timestamp (note paragraph [0036] of Rail).

For claim 4, the combination of Shrader et al., Rail and Shibata et al. teach a method of claim 1, wherein the step of receiving the user ID more specifically comprises receiving the user ID through an HTML page (note column 5, lines 44-47 of Shrader et al.) that is communicated from a remote client browser (note paragraph [0021] of Rail).

For claims 8, 20 and 23, the combination of Shrader et al., Rail and Shibata et al. teach a method of claims 1, 17 and 21, wherein the step of accessing the encryption key more specifically comprises retrieving an encryption key from a storage segment containing a plurality of encryption keys (note column 7, lines 20-23 of Shibata et al.), wherein the retrieved encryption key is obtained from a location or position within the storage segment based upon the index number (note column 18, lines 54-64).

For claim 11, the combination of Shrader et al., Rail and Shibata et al. differ from the claimed invention in that they fail to specify the encrypted message is converted into an ASCII string using a "printf" command.

It would have been obvious to one of ordinary skill in the art to convert the encrypted message to an ASCII string using a "printf" command because it was well

known in the art that the printf command returns an ASCII string when printing an integer using the "%c" conversion specifier.

For claim 12, the combination of Shrader et al., Rail and Shibata et al. teach a method of claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically includes converting the encrypted message into a hexadecimal value (note column 6, lines 43-47 and FIG. 7 of Shrader et al.).

For claim 18, the combination of Shrader et al., Rail and Shibata et al. teach a method of claim 17, further including a system to generate an expiration timestamp (note paragraph [0032] of Rail).

For claims 19 and 24, the combination of Shrader et al., Rail and Shibata et al. teach a method of claims 17 and 21, further including a system configured to communicate the ASCII string to a remote computer (note column 7, lines 33-36 of Shrader et al.).

For claim 25, the combination of Shrader et al., Rail and Shibata et al. differ from the claimed invention in that they fail to specify the step of communicating the ASCII string to a person through voice communications.

It would have been obvious to one of ordinary skill in the art at the time of the invention to communicate the ASCII string to a person through voice communication. It

is common practice to recite pieces of information (passwords, social security numbers, credit card numbers) over the phone to authenticate an individual to a service providing entity. For example, when a home security alarm is activated, the alarm company will call the homeowner and require a password to be recited in order to authenticate the homeowner and establish the alarm was a false positive.

3. Claims 3, 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail and Shibata et al. as applied to claim 1 above, and further in view of Berners-Lee et al. and Verio.

For claim 3, the combination of Shrader et al., Rail and Shibata et al. teach a method of claim 1, further comprising passing the ASCII string to a remote computer using FTP (note paragraph [0021] of Rail) within an HTML page (note paragraph [0024]) of Rail).

The combination of Shrader et al., Rail and Shibata et al. differ from the claimed invention in that they fail to specify the ASCII string is passed in an FTP URL being of the form ftp://ID:ASCII@hostname, wherein ID is the user ID and ASCII is the ASCII string.

Berners-Lee et al. teach "URL schemes that involve the direct use of an IP-based protocol to a specified host on the Internet use a common syntax for the scheme-specific data: //<user>:<password>@<host>:<port>/<url-path>" They go on to specify that <user> and <password> as "user: An optional user name. Some schemes (e.g.,

ftp) allow the specification of a user name. Password: An optional password. If present, it follows the user name separated from it by a colon."

The Verio glossary defines password as "A series of characters that enables someone to access a file, computer or program." This definition would make the ASCII value a password because it is a series of characters that are enabling a user to access files on an FTP server. It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail and Shibata et al. passing the ASCII value in an FTP URL because Berners-Lee et al. teach the convenience of passing user ID's and password values to an FTP server through the URL.

For claim 14, the combination of Shrader et al., Rail and Shibata et al. teach a method of claim 3, further including the step of passing the index number to the remote computer (note column 19, lines 13-43 of Shibata et al.).

For claim 15, the combination of Shrader et al., Rail and Shibata et al. teach a method of claim 14, wherein the step of passing the index number to the remote computer more specifically comprises passing the index number to the remote computer separate from the ASCII string (note column 19, lines 13-43 of Shibata et al.).

4. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail and Shibata et al. as applied to claim 1 above, and further in view of Jenkins.

For claim 5, the combination of Shrader et al., Rail and Shibata et al. differ from claimed invention in that they fail to specify the message digest of the user ID more specifically comprises computing a four-byte binary value.

Jenkins teaches a hashing function that "Returns a 32-bit value." Note that a four bytes value is equal to 32 bits.

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail and Shibata et al. that used the four byte hashing function of Jenkins to create the user ID message digest because Rail teaches to use "a suitable hashing function" and Jenkins teaches his hash function is "faster and more thorough than the one you are using now."

5. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail and Shibata et al. as applied to claim 1 above, and further in view of Krishnaswamy et al (U.S. Patent 6909708).

For claim 6, the combination of Shrader et al., Rail and Shibata et al. differ from claimed invention in that they fail to specify the expiration timestamp is computed in Epoch format.

Krishnaswamy et al. teach a communication method that "records timepoints in the epoch time format."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail and Shibata et al. that computed the timestamp in Epoch format because Krishnaswamy et al. teach "This

embodiment solves the problems associated with converting to and from daylight savings time because daylight savings time is a local time offset and does not affect the epoch time. Furthermore, the timepoints in epoch time format require less space in the call record than they do in local switch time format."

6. Claims 7, 10 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail and Shibata et al. as applied to claim 1 above, and further in view of Tan (U.S. Patent 6,490,353).

For claim 7, the combination of Shrader et al., Rail and Shibata et al. differs from the claimed invention in that they fail to specify the index number used to access the encryption key is randomly generated.

Tan teaches a key management scheme where "it may select these [key start points and lengths] by randomly selecting table entry numbers."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail and Shibata et al. with randomly selected index numbers for the added security of an unpredictable sequence of encryption keys.

For claim 10, the combination of Shrader et al., Rail and Shibata et al. differs from the claimed invention in that they fail to specify the step of concatenating the index number to the encrypted message.

Tan teaches a key management scheme where "the seed (randomly generated index number) may be communicated as part of the message transmission."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail and Shibata et al. which included the index number in the message transmission as a convenient way of storing the index number so the server would not have to locally store which cookie is encrypted with which key. It is well known in the art that an easy way to include two pieces of data in one message is to concatenate the two pieces of data together.

For claim 13, the combination of Shrader et al., Rail and Shibata et al. differ from the claimed invention in that they fail to specify the encrypted message and index number are converted into an ASCII string using a "printf" command.

It would have been obvious to one of ordinary skill in the art to convert the encrypted message to an ASCII string using a "printf" command because it was well known in the art that the printf command returns an ASCII string when printing an integer using the "%c" conversion specifier.

7. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail and Shibata et al. as applied to claim 1 above, and further in view of Jenkins and Krishnaswamy et al.

The combination of Shrader et al., Rail and Shibata et al. differs from the claimed invention in that they fail to specify the encrypted combined message digest and timestamp are an eight-byte binary value.

Jenkins teaches a hashing function that "Returns a 32-bit value." Note that a four bytes value is equal to 32 bits. Krishnaswamy et al. teach an epoch timestamp that is stored in 16 bits.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use DES to encrypt the message digest and timestamp. Note, because of the block encryption properties of DES, an input of 48 bits (32 bit hash plus 16 bit timestamp) would result in a one-block output of 64 bits or eight bytes.

8. Claims 26-28 rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail and Shibata et al. as applied to claim 21 above, and further in view of Stern (U.S. Patent 6,110,044).

For claims 26-28, the combination of Shrader et al., Rail and Shibata et al. differs from the claimed invention in that they fail to specify the ASCII string is printed onto a ticket selected from the group consisting of an airline ticket, a concert ticket, an employee ID card, and an event ticket and further specifying the ASCII string be printed on the ticket in a form that it may be later electronically scanned for verification.

Stern teaches a ticket printing and verification method which "contains a barcode printer (or other means for embodying a machine-readable indicium in a payout ticket), which prints both alphanumeric and barcode information on a payout ticket, including a

validation number." Note that in this case, a payout ticket would be an event ticket because successful verification of the ticket results in a payout event. Stern also teaches, "Selection circuitry 105 may also contain circuitry for encrypting all or part of the barcoded data imprinted on the payout ticket."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail and Shibata et al., which printed the ASCII string on an event ticket with a bar code that can be electronically scanned because Stern teaches a method for securely producing and verifying monetary payout tickets.

9. Claim 16 rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail, Shibata et al., Berners-Lee et al. and Verio as applied to claim 14 above, and further in view of Tan.

For claim 16, the combination of Shrader et al., Rail, Shibata et al., Berners-Lee et al. and Verio differs from the claimed invention in that they fail to specify converting the encrypted message into an ASCII string more specifically comprises converting a combination of the encrypted message and the index number into an ASCII string, wherein the index number is communicated to the remote computer as a part of the ASCII string.

Tan teaches a key management scheme where "the seed (randomly generated index number) may be communicated as part of the message transmission."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail, Shibata et al., Berners-Lee et al. and Verio which includes the index number in the message transmission before it is converted to an ASCII string as a convenient way of storing the index number so the server would not have to locally store which cookie is encrypted with which key.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David J. Pearson whose telephone number is (571) 272-0711. The examiner can normally be reached on Monday - Friday, 8:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER